MONTREAL – GNSO - EPDP Phase 2 Meeting (2 of 4)
Sunday, November 3, 2019 – 17:00 to 18:30 EDT
ICANN66 | Montréal, Canada

UNIDENTIFIED MALE: It is November 3, 2019 at 5:00 P.M. This is the GNSO EPDP Phase 2 meeting, 2 of 4 in Hall 511C at ICANN 66 in Montreal.

[The recording has stopped.]

JANIS KARKLINS: So good afternoon. Or rather, good evening. If I may ask team members to take their seats, we will start in a minute. I am giving 30 minute notice for recording because usually Terry gives us a minute notice for recording.

[This meeting is being recorded.]

JANIS KARKLINS: So shall we start? So once again, good afternoon. Welcome to our second meeting of, in the framework of Montreal meetings. So today we have basically two things to do. First is to discuss a little bit how we will approach tomorrow's public session and after that, to go back to our brand-new and plow through remaining building blocks. Hopefully, we

will end all of them tonight and then we will go tomorrow, enjoy the Montreal. No, I'm joking.

But on the first point, we circulated to the themes list proposed slide deck and I hope that you had the chance to look at them to propose slides. So basically, session will have a number of sort of modules. Keith will open the session, will do introduction. So I don't know. How can I move on?

Then I will make a presentation of our work, the approaches we're taking and where we're standing now. Then Strawberry Team will outline the progress and their activities. Then I will come back with sort of information about intended timeline and then we would go to Q&A session.

What I want to say, that in my introduction, I would go through kind of general elements explaining how we worked on use cases that led us to the creation of building block workstream and that building blocks will fall in their places as a policy recommendation once we will get to the initial report.

So then I will explain and outline what are those building blocks that we're dealing with, showing a nice picture of hamburger. And then I will outline maybe the most fundamental agreements we have reached by now and they are the ones that SSAD will be used by accredited entities and individuals that we will try to work on automation as far as it is feasible and legally possible, permissible. And the rest would be standardized and that accreditation does not mean automatic disclosure of the requested information.

So I think that these are those fundamental elements that we have agreed and that form the basis of our progress.

And then on the timeline, I will still introduce the premise that we are working on the initial report submission in early December that would allow us to review comments received during the end of January meeting of face-to-face meeting that we are planning in Los Angeles.

So again, I know that yesterday morning there was sort of some doubt about possibility of release of the initial report in early December. So if we make progress this afternoon and tomorrow and also Thursday so then maybe we can hope to do that by talking about maybe a few options of SSAD, not the final sort of architecture but just options. Yeah, but that is for our discussion on Thursday when we will see how far we have gotten with the building blocks.

And then also what is important is that we would seek input from community on those five questions that are now outlined on the screen, hoping that we would sort of tap in collective wisdom of the community and get some advice and new elements that we may have overlooked collectively. So again, these are just guiding questions, not the ones we would insist that those who will take the floor should focus on. Nevertheless, it is better to provide those guided questions rather than let completely unstructured conversation.

So this is outline of presentation and if there is anyone [inaudible] in disagreement with that type of approach, with elements that are included in the presentation, now would be the right time to spell them

out. And I am in the Zoom room if you want to use that. Otherwise, lift your name plates. The floor is open.

Yeah, and of course, I understand that the session would be more for community, not for team members to intervene. Of course, I cannot prevent anyone from speaking but I think that this would be very useful for us to listen, community input as much as we can. So the floor is open. Thomas.

THOMAS RICKERT: Thanks, Janis. So I do like the presentation. I was just wondering are you solidly looking for community input so that we receive input from the audience, or is this also an opportunity for the audience to ask questions?

JANIS KARKLINS: No, no. Also audience ask questions, questions of clarification, conceptual and I will try to answer as much as I can, and if not, then of course, any team member will be invited to join the conversation. And again, I will not try to outline anything that we have not discussed or I am not sure where we're going. So I will be more reserved in speculating what would be the outcome of our conversation.

THOMAS RICKERT: Just to be clear, I fully trust that you are doing the right thing. I was just wondering if it was going to be direct, by direction or whether we are just seeking input from the community.

JANIS KARKLINS: So actually, that's a question to keep because he will be running the show.

KEITH DRAZEK: Great. Thank you very much.

Hi, everybody. Keith Drazek. Yeah, so just a little bit of context. This was originally proposed as a plenary session by the GAC and as the GNSO Council and the GNSO is responsible for managing this particular PDP, I stepped up and offered to engage with Manal and the GAC colleagues who put the initial plan together and volunteered to moderate. So I'm essentially going to be the moderator tomorrow. We will have Q&A.

I think this was initially intended to be, or is intended to be, an update to the community, the opportunity for the community to ask questions. Certainly, if there are questions that can be answered at the time, great. If we need to take those questions offline in a way and come back to the community, we could do that as well. But I see this as a dialogue, an opportunity for an exchange from the EPDP team and with the community. And so I don't think we have an idea that it needs to be overly structured in one way or the other. I think it's a reasonable question, Thomas, in terms of just understanding what to expect and anticipate. So I'm happy to hear any thoughts that you all may have as well.

One of the things that, as you'll go back to the blocks of discussion, is for the community to provide input on the importance of a Uniform

Access Model as it was discussed, now being referred to as an SSAD. But yeah, I sort of see this primarily, number one, as an update and then an opportunity for that dialogue or Q&A between the community and the team. I hope that's clear. If it didn't answer your question, I'll try again.

JANIS KARKLINS: Thank you, Keith. Margie, you're next in line.

MARGIE MILAM: Is there going to be – maybe that's the slide – discussion about the paper that was submitted to the Data Protection Board and how it affects our timing? Because it seems like that's an important development to weave into the presentation.

JANIS KARKLINS: Yeah. No, as I mentioned the Strawberry Team will make a presentation. So that will be part, one of the elements of the structure of the session. Marc Anderson, please.

MARC ANDERSON: Thank you, Janis. So I put in Zoom chat, potential rephrasing of the third and fourth bullet points for consideration. I can just read it real quick. On the third bullet point, is there anything else the EPDP team should consider with third party identity providers? I think that's more in line with the language we had yesterday around identity providers and a little bit closer to, I think, the conversation we had yesterday.

And then on the fourth bullet point, I put in what financial considerations should the EPDP take into account for the development and maintenance of the SSAD? I think that's a little bit more of a generic statement than the one that's currently in there. So just some potential alternative language for consideration. Otherwise, I think the presentation looks good. Thank you.

JANIS KARKLINS: So thank you, Marc, and also thank you for your editorial proposals. Milton, please.

MILTON MUELLER: Just to express support for Marc's reworking of bullet point number four and also, on the slide about the Strawberry Team, are we being careful to differentiate the Strawberry Team, not necessarily the Strawberry Team, but the UAM model developed by the ICANN Org from the model that we're developing?

JANIS KARKLINS: I'm sorry. Could you repeat the question?

MILTON MUELLER: I think many people are going to be confused about the relationship between what the Strawberry Team has put forward as a model and that it is not necessarily the same as the model that we're working on. So I hope that the presentation makes that distinction clear.

JANIS KARKLINS: Yes. I will make presentation as you saw, on the Hamburger model where UAM is one of the options that we may consider but not the only option that we're considering.

MILTON MUELLER: But that's exactly what I'm concerned about is that you can have a unified system that is not necessarily the same as the one described in the Strawberry Team document that was sent to the EPDP. So showing them a picture of a hamburger doesn't necessarily answer that question. I think we need to make it very clear that the process by which the Org developed this UAM model and is taking it to the DPV is not necessarily the same as our process.

JANIS KARKLINS: Yeah, I think so. That will be said. [Elena], could you confirm that?

[ELENA]: Yes, of course, and I can point out this distinction when I begin with the presentation and make sure it is understood that this is something that Org hypothesized, nothing to do with. Thank you, Milton.

JANIS KARKLINS: Okay, thank you. Alan Greenberg, please.

ALAN GREENBERG: Sorry. [Elena] just said what I was going to say. Just we have to make it clear it's a hypothetical model proposed by Orgs for the purpose of talking to the Data Protection Board, not necessarily the one we're deriving.

JANIS KARKLINS: Okay, thank you. So I understand Marc and Tom's hands are old or new? Please.

THOMAS RICKERT: Yeah. I'm not sure whether you've made that point earlier, but I think what we should probably agree on as a group is that we will not use this session as a front to relitigate positions because I think it's not going to be balanced if we start that. And so I think Janis, you know the status of our discussions inside out so I would prefer we leave the responses to you and if you think that you need to reach out to any of us for details, then you can manage that process. But I think it wouldn't be good for any of us to put ourselves in the queue and try to advocate their respective policy positions.

JANIS KARKLINS: Yeah. No, I will do my best. I will do my best and I think that the way, how Keith maybe formulated and proposed, if there is no clear-cut answer, then maybe we can promise to come back and provide answer at a later stage or directly, through direct communication after the session.

So good. I understand that there is some editing going on in the chat room and so we will use the outcome of that process in the slide.

So I have no more questions, comments. I take that we are on the same page and we can move to the building block.

Yesterday, we started our conversation about [query] policy and we couldn't get beyond A. No actually, we got beyond A but we got stuck on the non-exhaustive list and we formed a small group of I would say most interested parties and tried to reformulate and get to agreement among those who were part of that group, and the text on the screen now is the one we collectively came up with. And I would like to see whether this proposal would now meet support of the team as a whole.

The text was circulated last night also for your review and I hope that is not coming as a surprise to you.

Brian?

BRIAN KING: Thanks, Janis. We can start the party here. It looks like this really depends on who the entity is that's disclosing the data and I think this language gets a little odd if we're to assume that the contracted party is the one disclosing the data, especially monitor the system and take appropriate action such as revoking or limiting access. How could the contracted party do that if they are the entity disclosing the data? How could they revoke or limit access to the SSAD? It didn't seem to make sense to us when we took a look at it. Thanks.

JANIS KARKLINS: Marc Anderson, please.

MARC ANDERSON: Thank you, Janis. Just a quick thanks to the small drafting team that came up with this new language on behalf of the registries who looked at it and we have no issues with it.

JANIS KARKLINS: Answering Brian's concern, I think there was no specific sort of indication who would be making disclosing decision. It was simply an abstract that SSAD should, right? So again, if we will come up the model where this sentence does not make sentence from operational perspective, but for the moment as a matter of principle, we felt that this would be something we could agree on. So that would be my comment.

Nothing is agreed until everything is agreed and as I mentioned, so once we'll go put initial report, we will do kind of a reading of consistency as well with what is put together makes sense because we are working now on the building blocks slightly in isolation. Each of them make sense by itself, but once we will put together, we will need to look inconsistency and that is what we will be doing. So James, please.

JAMES BLADEL: Hi, Janis. Thank you. And I was approached with one note here in the top where we qualify that requests are not legitimate and of an abusive

nature. One of the changes that I think we'd like to propose is that that "and" become an "or" and that they would be not legitimate or of an abusive nature.

And I think that the concern was originally that we had to meet both tests in order to essentially consider something abusive whereas what we're essentially saying now is that it would be abusive if either of those conditions were met and so that's one of the changes that we'd like to propose. But otherwise, perfectly fine with the new revised language that we came up with in the small group yesterday. Thanks.

JANIS KARKLINS: Yeah. No, I think that makes sense and probably this was the meaning of our discussion yesterday so either we put "or" or "and/or". That would be the [inaudible]. Marika?

JAMES BLADEL: "And/or" is also acceptable.

MARIKA KONINGS: My recollection of the small team discussion was that the "and" was important, that both those criteria would be met in order to be determined abusive.

JAMES BLADEL: So if I may respond, the "and" was important when the list was expansive and squishy, and I believe since the list is narrower and

tightened up, I'm trying to understand it. We can put together a two-column truth table here of requests that are legitimate and abusive. We would still take action against those. We could put together a truth test of not legitimate but not abusive. We would take action against those. So I think the "or" fits when you look at it from the perspective of a truth table. It does allow for either test to be made, but I think that because we have a tightened, smaller and narrower list below, it is a more effective filter. But I'd like to hear why that doesn't work. What is the scenario where something is legitimate and abusive but we don't want SSAD to act on it? Or the other way around, that something is illegitimate but not abusive.

JANIS KARKLINS: So would Alan and Milton intervene on this or I will take Margie first, before? Margie, please.

MARGIE MILAM: Sorry, that's the bad mic. No, we were firm on the "and" and I think the problem is if you look at some of the points, like say, four, sending high volume requests. We're very firm on the BC side that high volume is not necessarily abusive and I think you could read it that way without the "and". The reason we were okay with this is because we started from the premise that the requests are not legitimate and that was the key to accepting the list from one through four.

JANIS KARKLINS: But also, we clearly, we looked at examples and that's why, also, this automated appeared in the text of the list so that clarified what we meant by this high volume. It's not the high volume per se but high volume, machine generated high volume requests.

So I have now Brian on the same topic. Brian?

BRIAN KING: Thanks, Janis. I think that what's hanging me up is the possibility that if a request is deemed not to be legitimate, it could somehow result in de-accreditation or revoking or limiting access based on who knows whether a request is legitimate and who decides that and what are the thresholds for legitimate. I like what we've done with abusive, but legitimate or abusive just seems to be way too broad. It needs to be "and". It just can't be "or" because legitimate is way too squishy. It would just undo everything that we've done to pin down what abusive means. Thanks.

JANIS KARKLINS: I think there is also a good understanding last night that we were talking about accredited entities, not just anyone from the street, random person. So that also, this understanding helped us, at least yesterday to get on the same page.

Would Alan like to intervene on this one or something else? So then I will keep both of you on that. I will take now Volker, then Hadia and then Mark [inaudible].

VOLKER GREIMANN: I think there is a couple of qualifiers that should make it clear that there is no issue with an "or" in this case. I mean, first, it has to be clear that the requests are not legitimate. That means not that someone may think that, "Well, maybe this is, so we'll do something here." This has to be basically, prima facie, clear that this is not a legitimate request. And for the high automation, there is also a number of qualifiers there.

I mean, ultimately, if someone is coming at this SSAD with pure intentions, then they shouldn't have a problem. If anyone in this room is trying to make, later on, requests that are not legitimate or intends to file such requests or requests that are abusive, then they shouldn't be using the SSAD in the first place. So if you are doing this in good faith, then an [inaudible] should not be a problem here.

JANIS KARKLINS: Hadia, please.

HADIA ELMINIAWI: So again, I would like to, we [fair] here that the problem yesterday was not initially with the list itself, but the problem initially was with a legitimate request being mistaken and considered an abusive request. And that's why I think that "and" is important because it ensures that legitimate requests are not and could not be mistaken for abusive requests. And my question is if you have a legitimate request, could it be abusive and again, "and" solves a lot of the main problem that we were facing. And again, the main problem was not the list. The list, to

me, was fine and you modified it now and it's fine as well. But the problem was with the good requests being mistaken as bad ones.

JANIS KARKLINS: Thank you.

ALAN GREENBERG: A point of order. Have we ever defined what "legitimate" request is? Abusive, we describe here. Do we know what that word means?

JANIS KARKLINS: So that's a question to the team.

JAMES BLADEL: We have not defined that. And that's what Brian King was just pointing out.

JANIS KARKLINS: Okay, let me take Mark Sv.

MARK SVANCAREK: Thanks. Mark Sv. Well, Alan just stole my first point which is I don't think we have a definition of "legitimate". So the idea that we'll know it when we see it doesn't really hold. So I don't want to have to come up with another list. Here is the list of abusive and here is the list of legitimate.

I just also wanted to make just a clarification to something that Janis said about the use of the word "automated". The use of the word

"automated" was inserted into number one and number two, specifically but it wasn't intended to necessarily apply to all of these points. Certainly, if I am making a high volume of legitimate requests, there may be some automation involved on my side, something that's not defined here and not really in the scope of this EPDP but it could be automated and we don't want to send an expectation that we would never use any automation on our side of the pipe. Thanks.

JANIS KARKLINS: Please, [inaudible]. Yeah, please go ahead then. You were in line for a long time already.

MILTON MUELLER: So I really think we're getting stuck on a word game here. It's clear from number two in the definition of abusive, high volume automated duplicated requests that were previously fulfilled or denied, so those were presumably legitimate requests, particularly if they were fulfilled. So what we're trying to do with defining abusive here has nothing to do with the legitimacy of the request but with the behavior of the requesting process.

We're trying to stop gaming the system and it seems like "abusive" almost by definition means illegitimate in some sense. And I think we could actually just delete the word "legitimate" because how do you know the request is not legitimate until if you're inundated with high volume submissions of malformed or incomplete requests? What does it mean to be illegitimate in that context?

I think, really, the people who want the "and" in there have not answered James's basic question. What is a legitimate and abusive request? Because you would permit those. You would permit abusive requests that were somehow legitimate. So what do you propose to do about that?

JANIS KARKLINS: So please, think about Milton's proposal. If we delete "are not legitimate and that the requests are of abusive nature" and just leave it there. So maybe that would be a way forward. James, what do you think?

JAMES BLADEL: Thank you, Janis. And I think we were kind of headed in the same direction as a thought was that if we haven't defined legitimate and I don't know what legitimate looks like and I can't police illegitimate requests because I don't know what those look like either, I think it puts the implication there is no such thing as a legitimate request that is also abusive. And that's kind of where we were trying to go here. So if we take out "legitimate", then it essentially says if these requests are clear, demonstrated or clear – I'm not really married to either one of those – but that it is clearly of an abusive nature and abusive nature follows this recipe down below, then I think we're okay.

My question is if we don't and we have to have legitimate, then the two questions are 1) How do we define legitimate, and 2) I think that was Mark Sv's point, so sorry to steal your thunder on that. But how do we

define legitimate? How do we tell when something's illegitimate because it seems like it's reading intention?

And then the second part is how do we handle a legitimate but abusive request, something that is, I guess I'm having trouble wrapping my head around that but if something falls into that definition that it's both legitimate and abusive, then this list says we have to take action and I don't know how to determine that or what action to take. So that's why I'm kind of getting wrapped around the axel here a little bit.

JANIS KARKLINS: So let me ask Margie. If we take out "legitimate" out of this [shuffle], would that be acceptable to you?

MARGIE MILAM: No. No. The problem is it depends on who the disclosure is, I guess. If the disclosure is ICANN, it's probably less of an issue than if it's a registrar or registry where there's a disagreement over whether the request is proper. And this is a scenario we see today. We see legitimate requests being denied. And what I'm trying to avoid is a situation where there's a good faith reason to submit the request, the registrar doesn't accept it, and there happens to be a lot of them because if there's a cyber security event or there's a lot of domain names, that's where you get the high volume.

And so what we're trying to talk about here is really when there's a good faith request that has been submitted by a requester and for whatever reason, the registrar or registry doesn't agree with the legal basis but

there's high volume, I don't want that to be defined as abusive. So the volume in and of itself should not be a problem. It's where what I thought we were talking about yesterday was situations where it was high volume spam, just there wasn't any good faith associated with it and that's why I was comfortable with the legitimate as part of the lead-in. And so that's the concern I have.

JANIS KARKLINS: No, we are not talking here about the purpose or examination of the purpose of the request. We are talking about limitation of the numbers if there is obvious [gaming] of the system. So that's the main point. We were talking about purpose as another building block and I think I understand your concern but this is not in this place where this concern should be addressed.

MARGIE MILAM: Okay. I just can't move it. But I think standing alone though, the scenario that I'm talking about where there are requests that are sent in good faith and there's a lot of them would technical fall under this definition of abusive and that's why this language is too broad.

I was fine with it when we had the legitimate and I'm happy with the discussion about what is legitimate. We could certainly define it. I agree with the observation that it's not defined, but I do have, if we're not going to have legitimate, then we have to go back and narrow this because it implies that having high volume requests that are legitimate

that somehow cause an SLA to fail is abusive. And what you're talking about here is potentially revoking someone's accreditation afterwards.

JANIS KARKLINS: No, Margie. No. Look, it says yes but what we're talking about here is high volume automated submissions and then we need to read all sentences, not only beginning. So "not informed and incomplete requests".

Would any, let's say, serious organization or researcher would send half-baked proposals every millisecond to the system and in high volumes? Or would anyone send, legitimately send the same duplicative requests in an automated way which have been already answered or denied every millisecond, as we discussed yesterday? So that was put all in description demonstrating what was meant by abusive nature. So that's …

MARGIE MILAM: If I could reply, there's no time limit on these. If we had a time limit on that, then I think it does alleviate my concern. But high volume during what time period is not addressed in this list. So that probably would satisfy my concern.

JANIS KARKLINS: What is your proposal? Your time limit?

MARGIE MILAM: Volume, I guess I'd ask the SSAC folks, do you have a sense for what? Or Marc?

JANIS KARKLINS: Let me take Alan who has long time in line.

ALAN GREENBERG: Okay. I put my hand up for a completely different reason but they seem to have merged now.

My original account was going to be the lead-in sentence, I think is inappropriate for two different reasons. That is "The EPDP recommends that the entity disclosing the data". Number one, for many of these abusive requests, no data will ever be disclosed so we have to consider that. Also, in any realistic SSAD, whether we end up using a single entity that then funnels requests to contracted parties or perhaps answers them all itself if it's ICANN or some combination of that, the detection of the abuse is going to be not at the disclosing level but at the receipt level. So it's the first entity that sees a lot of progress.

Because remember you could have a huge volume request that are scattered over many different registrars and no registrar is going to see a high volume, but the overall entry into the system may be abusive and inappropriate. So I would suggest that if we're talking about entry into the system, it's the volume that counts there or it's the volume over what period of time. It has nothing to do with the legitimacy of the request itself. It loses Volker's point of duplicate requests which we may have to cover somewhere else.

But really, we're talking about you're having a service which is being inundated unreasonably and so if we remove the whole issue of the discloser of the data and just look at it as how do you, as a system designer, make sure someone doesn't abuse your system regardless of what the details are, I think we can probably come up with language that works. Thank you.

JANIS KARKLINS: Now look, we are working here on the assumption that since we do not know who will be disclosing data, that's why there is this generic term saying whoever will be disclosing data needs to follow those policy recommendations. And then is maybe we need also to whether Point B should also be swapped with Point A where initially, you monitor and then you take measures.

ALAN GREENBERG: My point was it's irrelevant who ends up disclosing the data if data is ever disclosed because in many cases, it may not be disclosed. It's really, are we abusing the entrance part into the system way before data is disclosed or before the evaluation is even made? Thank you.

JANIS KARKLINS: Yeah. Volker.

VOLKER GREIMANN: You may know that in our company, I manage the team that deals with the abuse cases and I regularly look into the abuse queues that we have.

One thing that we see regularly is requesters that send requests for domain names that are not even registered with us. So we get the request, ten a day, which arguably is not a very high volume request for various links on a certain domain name that's not registered with us. We know that requester. We've tried to contact him and tell him to maybe adjust their scripts. They won't. When we see those tickets now, they just get closed and thrown in the junk queue.

Those are, in our view, requests that are clearly or demonstrably not legitimate but not abusive. Therefore, we need some way of stopping some way of stopping such requesters from spamming our queues with their requests.

I would propose that there should be some form of redress that when we limit the number of requests that somebody is sending because we deem them to be nonlegitimate, we have to provide a reason for that if we do that and they can then go to ICANN Compliance and say, "Hey, what's the problem here?" and then we'll work with them and work the thing out. But we do need the ability to filter those out because otherwise, other requesters, we have other people like that so it's not just that one. It's multiples that just send those requests in that we can't do anything with, requesters that only send their requests in Russian. Very nice. Don't know what to do with that. We don't [inaudible]. We ask them to send them in English. No response, but we get them five a day. We need to be able to filter those out and that's our request that are non-legitimate and we offer a form of redress for those so you can reestablish your full throttle access if you need it. But we need to have

both functions, the non-legitimacy and the abusiveness in the "or" version. Thank you.

JANIS KARKLINS: Okay, thank you. Let me take Chris now followed by Georgios.

CHRIS LEWIS-EVANS: Thanks. I don't have a massive problem with one, two, and three. I think the big thing that's causing issues here is number four in with the case with the "and" and the "or" section, and trying to solve this is maybe difficult. But I was just thinking that, really, what we're looking for here is intentional abusive nature. So I wonder if just inserting the word "intentionally causing SSAD or other parties to fail SLA performance" might be an improvement in helping that aspect.

And then why I raised my hand originally is the violation sentence at the bottom. I think we've discussed in other building blocks about graduated recourse or penalties, whether we can just change that language to be in line with other language in the building blocks to be graduated penalties rather than just going straight for a suspension. Thank you.

JANIS KARKLINS: Okay, thank you. Georgios?

GEORGIOS TSELENTIS: Thank you. Although I agree with what Chris said about intentional, I think it's very difficult to put words like this because somebody has to judge that. How do we judge the intentions of somebody who is using the SSAD?

On the other hand, the more we discuss here, the more I see that maybe I missed something in the discussion, that when we talk about, number one, high volume automated submissions of malformed or incomplete requests, here I don't see issues with the high volume, I don't see major issues with the automated that we can see there. I think the abuse is in the repetitive nature when somebody makes requests, like I mean, we said it. I think it was James who said, "It's like a broken record. I want that, I want that, I want that," and then we are trying to force the system to give us a response despite the fact that we do not put the right request. IT's malformed or it's incomplete and we are trying by repetition to break into the system and that consists the abuse. So I would suggest there to put something about the repetitiveness of the request and not insist so much on the high volume or the automation.

JANIS KARKLINS: Okay. What shall we do then? We have Mark Sv in line and then Alan and then Brian. Mark Sv. But please try to propose some way forward as you see it.

MARK SVANCAREK: I was hoping there'd be other people in the queue ahead of me because I was trying to come up with some language. I do see finally the point

that Milton and James are making, the truth table point about the not legitimate and abusive, that if it's legitimate but abusive, then the whole thing doesn't work. So okay, so I get the point there.

I am glad that we're moving away from intention because intention was a problem that I had yesterday and we managed to expunge that, so I'd like to keep that out if possible. But I don't have any good language yet, so please. I'll put my hand up again when I do.

JANIS KARKLINS: Okay, thank you. Let me then take Alan, Brian, Thomas and then maybe we can move on and then revisit at the end of the session while thinking about a possible fix. Alan, please

ALAN GREENBERG: Okay. I think James's example of someone who gets continually rejected and asks the same thing, and Volker's several examples of types of requests that are problematic are both valid and we need to address them.

I really think we need to do it in two completely separate sections because the high volume abusive, trying to make sure you don't meet an SLA or any combination of that is a very different problem from stupid people who send in things and get in your way. Ten requests a day in Russian are a pain in the butt, but it's not going to stop you from meeting your SLA.

Okay, so they're really two different things and if we try to cover them in two different ways, we may come to success. Trying to merge them into the same set of sentences is not going to do it. Thank you.

JANIS KARKLINS: What's your proposal, Alan? Can you formulate a proposal?

ALAN GREENBERG: I would scratch this all and start again, trying to make two different lists to cover the types of things we're talking about but not merge them in the same list, in the same paragraph.

Among other things, the high volume, I think has to be filtered out at the first entrance into the SSAD regardless of who's going to be answering the thing. The other ones are going to be detected by whoever is actually answering the query. So I think they're two different things and I suspect. I can't fabricate two paragraphs on the fly, but I think if we try to do it as two separate tasks, I think we'll come to closure pretty easily.

JANIS KARKLINS: Okay, thank you. Brian.

BRIAN KING: Thanks, Janis. I got a proposal. So I think what we seem to be concerned about in this relative group is that high volume has historically been throttled for us and that's been a problem. And high

volume requests that are not abusive or not made in bad faith should not be used to throttle the system or to result in suspension or termination of accreditation and so it seems to be that what we're really concerned about that I think is not going to be a problem for anybody else is requests that are made in bad faith. Right? I'm going to have to disagree with Mark Sv here, I think maybe for a different reason. But if we do include that as a concept here, I don't know if it makes sense to replace legitimate or to add it in addition or let's see how the language looks. But the requests are made in bad faith and of an abusive nature, something like that. In the common sense term of abusive, we don't have a problem with that.

Abusive requests should be filtered out but the way abusive is defined captures the kind of stuff that we need to do sometimes. So I think introducing that element of bad faith is good on its face there, and then also, it in practice hopefully would require an engagement with the party that's submitting the request so that whoever is about to throttle or suspend or terminate then has to get into that kind of compliance loop, like, "Hey, what are you doing?" and engage in that "Why is this not in bad faith?" before somebody takes some further action to suspend or terminate the accreditation. So that's our proposal. Thanks.

JANIS KARKLINS: Thomas?

THOMAS RICKERT: Thanks, Janis. I think Alan is completely right, that we need to sort of give this a fresh start.

I think we have three different points that we want to cover and I haven't fully formulated it, but one thing is the disclosing entities need to protect themselves from high volume requests that might prevent them from fulfilling their SLA.

So the first point is that they should be entitled to throttle the requests to ensure that they can meet their SLAs. The second point is, and I guess that we don't have that here, that disclosing entity needs to report suspicious requests to the central unit if we have one because as Milton said – I think it was Milton- it may well be that the requests are affecting different registrars or different TLDs so that only the central unit managing the process can determine whether there is abusive behavior in place.

And the third aspect is that the central unit is then required, basically the burger bun in our model, is required to carry out an inspection of the requests and if there is abusive behavior, that should be sanctioned. And whether or not abusive behavior is present, we would then have our four bullet points. I guess if we separate it that way, we should cover all the concerns that we have discussed.

JANIS KARKLINS: Okay. James.

JAMES BLADEL: Hi, thanks, Janis. Trying to incorporate all of the feedback so far and trying to think of a way out of this. Just a couple of thoughts or responses.

First of all, I disagree with Thomas and Alan that we need to throw this out and start over or come up with multiple lists for different scenarios. I think that it's worth repeating that this was a non-exhaustive list. It was an exemplary list that said, essentially, "not limited to" so coming up with another list still has, presumably, that open idea that there are types of abuses that we haven't thought of yet, that we cannot necessarily account for so we can't make a list that says, "Here are all the nine, four, or 78 things that are abusive," because bad guys are inventing new ways to abuse things all the time.

If I could, the second bit is I'm concerned that there is, and I'm trying to think of how to express this, that there is a sentiment building that because someone has encountered this in the past, that means that it is not an effective definition of abuse rather than introspectively saying that maybe someone was, an organization or an individual, was making illegitimate requests in the past.

So saying that I've run into this before or we've encountered this problem before is kind of like saying I've tripped over a barbed wire fence before. Maybe you weren't supposed to be running in that field. It's not the fence's fault.

But anyway, setting all that aside, I think I have an idea, which is if we are to leave in legitimate and abusive and both tests need to be met before either the SSAD or the receiving parties can take action against

a user, then two things. One is we need a definition of legitimate and two, it should say "legitimate in the determination of the SSAD operator or the entity disclosing the data" because we can't say "because I feel my request is legitimate, I don't qualify for your anti-abuse mechanisms." That's the honor system.

Anyway, I'm trying to find a way out of this where we can keep the different things here but I'm struggling. I'm really struggling. Thanks.

JANIS KARKLINS: From the discussion yesterday, I had a feeling that we were heading towards a model where we would have one central gateway receiving requests. So that was my feeling. Where we do not have yet a common understanding where the decision on disclosure would be made, either at that central gate which probably would be ICANN if that is the case or at the level of 2000+ registrars. So that is unknown for the moment.

But what I felt that we had this common convergence that we would have one gate. So if that's true, then we can maybe start thinking in real terms so that somebody at that gate who will receive this request would verify credentials, will be the first to see whether that is a single request or that is, let's say, a multiple domain name request or that is high volume request. And that would be then depending on the model where they would start resolving, looking into those requests or start sorting that this goes to that registrar, this goes to that registrar and then sending them down.

So my point is that in the case of central gateway, there will be immediately a point where any kind of abusive, at least the first screening of any abusive requests will be done or I'm completely wrong. I'm just looking at the guys who now operate that system, so I think. So if that is the case, then in normal circumstances, the first screening would be done already at the gate no matter where the decision is made. Right?

So can we think of some kind of scenarios, as Alan suggested, for legitimate high level requests, how the query policy is and then obvious abusive high level automated requests that we identified? So maybe we can think in that direction and try to put forward, ask some few guys put forward a language that we could look at maybe tomorrow on this specific point. Just a suggestion.

For instance, if I would say somebody from registrars and then BC and then SSAC do kind of thinking in those terms. [Stephanie] [inaudible], or you want to say something? Or you want to participate in the drafting?

[STEPHANIE]: Yes, I think I'd like to participate in the drafting and I did have a question. I apologize for coming in late. You know the old double-booked problem.

Why does it matter whether it's automated if it's abusive? I mean, there's plenty of ways to automate without automating if you know what I mean.

JANIS KARKLINS: So can I maybe ask who would then be those? Stephanie volunteered. Ben? No? No, you're not. Marc? Who else? James? Yes?

JAMES BLADEL: Question, and it's more of a request. We seem to be stuck here and I think the approach that we've done in the past of getting this cross-section small team to work on it, I would ask because I think the SSAC folks – Greg is not here – but perhaps the SSAC folks could because I think they have some experience and some reports on what is and isn't abusive access of the system. Maybe they can help us out here a little bit in a way that everybody can kind of rally around. I don't mean to put you guys on the spot, but it would be awesome if you could rescue us from ourselves right now.

JANIS KARKLINS: The alternative would be that I would ask staff to do the drafting based on what we heard here around the table simply following the common sense approach and kind of human logic putting query policy and then we would put that language for discussion.

But of course, staff does not have in-depth knowledge in every aspect of operating the registrars or registries. So volunteers, are there any? Chris.

CHRIS LEWIS-EVANS: Thank you. Can I just ask a question? I think I might be having a bad day and it might be a Kindergarten question if James's was a school question yesterday. So here, we're talking about query policy and going on what you said, Janis, around we're talking about a centralized system, we have identity providers and authorization credentials. So by the time we get to this query policy, and this is where my head is struggling a little bit, we shouldn't allow any queries that are not legitimate at this point because every request will have already had its legal basis checked, made sure the forms have been correctly filled out, gone, made sure it has a purpose so it is a properly formed request before it gets to the point where it is a full query for a decision to be made.

So have we got to a situation where, effectively, the authorization credential as I understand Alex has detailed, has effectively failed for it to be not a legitimate request? And that's where I am struggling and I wonder whether that is causing us some issues here and we're talking about the full system and realistically, by the time we get to this point in the building block, we should have a properly formed legitimate request. Yes, they could still be abusive but where I am struggling is realistically, we are trying to weed out some of these non-legitimate requests before we get to this stage in the building blocks. So I just wonder if that helps us frame what we're trying to achieve here. Thank you.

JANIS KARKLINS: Probably we need to think in terms of how system would function and maybe describe the functioning of the system and then see what are those elements that would prevent systems from functioning normally. So that's the logic that I see we should proceed.

And so I have few further requests for those who have not spoken. Ben and Farzaneh, then followed by Thomas and Alan.

BEN BUTLER: Thanks. The reason that I'm hesitant, me and SSAC in general, are hesitant to try and rescue us from ourselves in this is because what I see happening is kind of from the two different sides of the argument, both sides are thinking about problems that they have had in the old system, i.e. getting the Port 43 who is getting buried by invalid requests and bots that rum amuck and that sort of thing. And the legitimate users who might have high volume, the small number of large companies who might have large volumes of queries every day, are concerned about stuff that's happened either in the old system or in the current system which was never intended to be the permanent system, i.e. they send in, call it, 10,000 requests in a day and get rate limited somehow. Securities have the same problem with kind of overly aggressive rate limiting in some cases.

I think both sides can fundamentally agree there have been problems in the past. The reason I'm hesitant to try and rescue us from it is there is no solution unless we're both willing to accept that good faith is going to have to be involved. We have to put away the problems we've seen in the past and accept that realistically, disclosures of data are going to

have to give the benefit of the doubt to legitimate companies that have high volumes and legitimate companies that have high volumes are going to have to accept that sometimes a rate limit might have to go in place and the flag is on the play and they have to go back and say, "Why did I get rate limited?" and the burger in the middle can adjudicate.

I just, I don't know what the solution is. I would not even attempt to try and draft language with all these lawyers around.

JANIS KARKLINS: So somebody needs to have the courage and put forward the language, ultimately.

Farzaneh.

FARZANEH BADIEI: Thank you. So I just, I don't have a solution but I also think that if we have the small team and then they go and want to come up with wording and also the list that we have here has, the wording is not acceptable to some and it is not complete and also the various nature of the problems that have caused us to come up with this paragraph, I think it's kind of impossible for them to come up with something acceptable.

I think Volker said something interesting, that we don't know what sort of problems are going to happen but we can have a redress mechanism that if they limit the access and number of requests due to some reason they provide the reason and then there will be a redress mechanism

and we can come up with a process for lifting that limitation, and so instead of coming up with all these lists and stuff, we just have simple wording of in cases where the disclosure has actually decided to limit access, they need to go through such a process to either continue having that limitation or revoke it.

JANIS KARKLINS: So thank you, Farzaneh. Margie and Alex.

MARGIE MILAM: That's an interesting concept, Farzaneh. Yeah, I think having some sort of redress goes a long way to, at least, I think bridging the gap between what we're talking about. So I'd like to think about that.

JANIS KARKLINS: Alex.

ALEX DEACON: Sorry, I'm writing a suggestion that may move the ball forward here. I didn't quite finish but let me give it a shot. What if we changed the first sentence, A, and instead of using "not legitimate", we used something like the following. So let me just read it here. I don't have my right glasses on.

So A would read, "May take measures to limit the number of requests that are submitted by the same requester if it is demonstrated that the requests are frivolous, nuisance or vexacious, and of an abusive

nature." And from what I understand – I am not a lawyer – that is the language used for Freedom of Information requests. Does that help?

UNIDENTIFIED MALE: [Inaudible] "or" at that point?

ALEX DEACON: Yeah. I don't know.

JANIS KARKLINS: So any reactions to Alex's proposal? Instead of legitimate, could you repeat those three nice words that you said instead of legitimate?

ALEX DEACON: I don't know if I can. Frivolous, nuisance or vexacious. Margie, would "or" work if those three? No. Okay.

I'll put it in the chat.

JANIS KARKLINS: Can we get them on the screen by any chance?

BRIAN KING: If I could …

JANIS KARKLINS: Yes.

BRIAN KING: Thanks, Janis. If I could just add one bit of color to that, the concept of why that might be helpful is because there is juris prudence and there's some background on what that means. Here it looks like we're trying to define abuse or trying to define legitimate and that would at least give us a concept, and the concept is that Freedom of Information Act requests in the U.S. are when you send requests to the government to produce publicly available documents, and so the government uses that standard to either allow the request if it's not one, two, three of those adjectives. Or there is some juris prudence around if you're really just being a jerk and trying to bury somebody in paperwork, then they can be denied.

So there's allegory there that we're trying to use to get us out of this inventing definitions pickle. Thanks.

JANIS KARKLINS: Okay, thank you for explanation. Can we get on the screen? And that would replace "not legitimate" and the "and" would stay in the middle. James?

JAMES BLADEL: Hi, thanks. So I don't mean to sound sarcastic or disrespectful but it sounds like we continue to come up with synonyms for abuse, so we're saying that something is abusive and abusive. Or abusive, abusive, abusive, and abusive.

And we're giggling and it's late and I'm sorry. But that kind of was the original, just to bring us back to the beginning and why I felt like we were safe, and I was mindful of the concerns that Margie had yesterday, that I thought we were safe and either putting an "or" there or taking it out is because I feel like legitimate – sorry, it's late – illegitimate is contained within the definition of abuse. So to me, I don't mean to come down hard on Alex's proposal and I appreciate the thought that he put into it, but if you kind of just take a step back and look at it from 10,000 feet, it looks like we're saying "abuse" in a lot of different ways and then we're putting bouillon operators in-between them and just, I feel like we're making work for ourselves. Thanks.

JANIS KARKLINS: So then we're coming to the thing. Let's, maybe, if you see Point B. So when we're looking, so following the logic that the central gateway should first of all monitor the system and take appropriate actions in case of abuse or misuse of the system. And I think that this is something that we agreed already. So the monitoring is needed.

So then the next step, logical step, would be after monitoring, is to take measures and this is where we're talking about in point A. Make measures to limit number of requests that are submitted by the same requester if it id demonstrated that the requests are of abusive nature. And then Asterix describing what that abusive nature is.

So maybe we need to address the issue of the, let's say, high volume requests that the system should be treat, or should be able to work with the high level volume requests that are not of abusive nature, that

would not fall under the description of abusive nature in a separate point.

So we are saying that when it comes to small number or individual requests that go through, it's not an issue. So they go through and are answered yes or no.

Then their security or infringement high volume request with the purpose and demonstrated purpose and not of abusive nature. So they also, the system needs to be able to deal with that type of situation from policy perspective. I don't know how technically, if he's [inaudible].

And then we are addressing issue of demonstrated high volume abusive. And then we have this language here. So maybe that is the way forward and I would try to formulate something for us tomorrow to look at, at those. Would that work?

So that's, then in the next 12 minutes to see whether we can get. So may I take that B is okay. Just making sure that we're fine with B.

So now let's go to the C. And so I have Farzaneh's and Chris's hand up. Would you lower them? Chris, please, go ahead.

CHRIS LEWIS-EVANS: Sorry, I put my hand up for B. I just put in the chat as well, I think before any action is taken, monitoring should come first so I'd like to suggest we swap B and A around in order.

JANIS KARKLINS: This is what I was tying to say, yeah, that would be the first we monitor and then we take actions. But that's kind of our logic. So let me see on C. Marika?

MARIKA KONINGS: Thanks. Here we had one suggestion to maybe, I think, it's more of a grammar thing so I hope it doesn't need much discussion, but move only to after respond so must respond only to requests. So I don't find any concerns about that or we can go ahead and make that Change.

JANIS KARKLINS: On C?

MARIKA KONINGS: Yes.

JANIS KARKLINS: could you repeat, please?

MARIKA KONINGS: So the suggestion that I think was made by Alex is to move only to after respond so that it would read "must respond only to requests for a specific domain name."

ALEX DEACON: This was just a grammar thing. I could live with it and I'm not an expert in grammar but it read better to me.

JANIS KARKLINS: Only grammar teachers are.

ALEX DEACON: Yeah.

JANIS KARKLINS: So any issue with the C. So then I take Daniel.

DAN HALLORAN: Just maybe it's late in the day. I'm just not sure what it means exactly, "Must only respond to requests for a specific domain name. What's the alternative."

JANIS KARKLINS: Okay. So then let us move. So is there anything else that comes to mind or we take others out?

And then so next sentence, responds to [inaudible] must not include more non-public data elements that have been requested by requester. Common sense, we agreed on that. But then the next sentence, let me see if we can agree on that. The response to a valid, legitimate request must include public data elements related to the domain name registration.

Conversely, the response to an invalid, illegitimate request must not include public data elements related to domain name registration. That

was also a result of our conversation that if we answer and take, or if the decision is made to disclose requested non-public data, then also elements of public data should be added to that request. But if the request is rejected. So then no data, even public data is not returned. Common sense kind of proposal. [Laureen]?

LAUREEN KAPIN: I'm sorry. I'm a bit confused. If it's public, why would it need to be disclosed? And if it's an illegitimate request, why does there need to be a response, and I'm sorry if I'm missing something.

JANIS KARKLINS: No, we had the conversation earlier, I mean, in one of the previous, saying that if turn is only nonpublic data, then the requester needs to go a second time to RDAP and seek public data.

So if the request is sent in and the request is responded favorably, so then the return is both requested public data and nonpublic data. But if the request is rejected, then no return is given. The system should not send the public data. So then the public data is available anyway. That was the logic of this proposal. Mark Sv.

MARK SVANCAREK: The idea was that if it's a bad request, no data will be returned. We didn't want to be in the situation where the disclosure then had to parse it out and say, "Well, I'll give you this portion but not this other portion." It's all or nothing. You either get, you have a good request and it's being

honored in full or you don't have a good request and no data is returned at all. It's just a cleaner thing.

JANIS KARKLINS: Yeah, that was the idea. Marc Anderson?

MARC ANDERSON: Thanks, Janis. I think I was going to say the same thing Mark Sv did. It was just no data. It's implied but just to be a little cleaner.

JANIS KARKLINS: Volker, are you in agreement?

VOLKER GREIMANN: Just one question here. I mean, looking at the real world implications of this, if a requester says that they are requesting data because they want contactability, they want to contact the data subject because of X, Y or Z, and it can clearly be determined that for that purpose, the street address or in other case, the e-mail address would be sufficient, then we might decide not to disclose the telephone number because that is not, you don't need the telephone number to send a letter to an infringer.

So we might still have a reason, a legitimate reason, to withhold certain parts of the information if the purpose stated does not require that information.

JANIS KARKLINS: No. That's right, but that is not what we're trying to say here. I think we, in one of the other points, we said that you cannot return more than is required. You can return less than is required but you cannot return more than is required. That is already fixed.

VOLKER GREIMANN: Yeah, I had it wrong in my head.

JANIS KARKLINS: Yeah. It's a late hour. I understand. So can I take Chris?

CHRIS LEWIS-EVANS: Thanks, Janis. I think this comes back to my previous point a little bit as well, and totally get what we're trying to cover off here but do we get to this stage in this building block where an invalid/illegitimate request actually gets through to this stage? Or do we say, illegitimate request must return no data and a reason why it is an illegitimate request? So blocking it off before it gets to a disclosing decision.

JANIS KARKLINS: No, sorry. I simply want to clarify that here, this is response to the discussions we had earlier, that if the response is no, so then no data is returned at all. But explanation, why? But that is given somewhere else. I think it's in the next building block. S here is saying, but if the response is yes, then you get both public data and requested non-public data. But not more than that. Simply to make sure that requesters should not

go to system twice, asking, getting nonpublic data and then going and then retrieving public data. Yes, please.

MARIKA KONINGS: I think to Chris's point, this may need to belong is the response requirements building block. It seems to be more appropriate there, and as you said, this is about query policy. I think this is a response requirement so maybe we just move it there. And I noted as well that Brian has suggested that we change, not include, the public data to replacing that with any data elements.

JANIS KARKLINS: Yeah. Okay. Can we get that on the screen?

Okay. So let me also reiterate once again that it's important for us to try to agree on principles and formulations. So once we stabilize that, then where it should go, in which part of the text, we will decide once we will have a logical reading of the whole recommendations. The important thing is that we agree in principle and then moving things around, we can do it as a result.

So may I take then that this part, as it now displayed on the screen, would be fine? Laureen?

LAUREEN KAPIN: Just perhaps a refinement and I totally understand the concern about not wanting to over-burden the system in response to an illegitimate request. That said, I think it would be useful to point to where the public

data is, not return the data but at least have something in the process that says, “This data is public and you can find it here,” because its public data so I don’t think we want to be shrouding or hiding public data. But I don’t think that the system should have to be burdened by parsing that out either. I’m sensitive to that concern, but I think there should be some sort of pointer. “Here’s where you can get this. It’s public.”

MARIKA KONINGS: I think that is something that probably addressed in response requirements. I think there is also something already in there that talks about if a request is denied, rationale needs to be provided. We need to double-check whether something of that nature is already there as well, but it probably belongs also in that building block, I guess.

JANIS KARKLINS: Alan, please.

ALAN GREENBERG: Thank you. The first part of the sentence clearly is needed because we decided consciously that we should include the public data so we don’t have timing problems.

The second half, we spent an inordinate amount of time talking about whether the response should include public data or not. I think we could have just left off that sentence and left it to the discretion of the

designer or each contracted party or whatever. We're just spending an awful lot of time on something which has no impact.

JANIS KARKLINS: Okay, and actually, we have run out of time. I have been reminded that the meeting is over. I would have be willing to spend even night with you, all of you. I'm not sure you would like to do it with me. It's so openly now. Okay, I'm joking.

So look, at least we have done this bit of a thing except the first day that needs to be added. I promise to try to formulate something for your consideration tomorrow and whether I will be able to send it tonight or tomorrow morning, meaning tomorrow by maybe 10, beginning of the public session remains to be seen but it will be in your mailboxes by 10 at the latest. And then we will take it up as a first item tomorrow at 3:15 when we are meeting again in this very room.

So thank you very much. This meeting stands adjourned, and please enjoy your evening.

[END OF TRANSCRIPTION]